TESTIMONY OF

Mr. Christopher Byron
Journalist
The New York Post

BEFORE THE
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 29, 2006

Mr. Chairman and members of the Subcommittee: It is an honor and a privilege to appear here today in support of H.R. 4943 ("The Prevention of Fraudulent Access To Phone Records Act), which makes acts in furtherance of so-called telephone records pretexting an explicit offense enforceable by the Federal Trade Commission. I suggest only that the act of pretexting for phone records should carry the heavier sanction of the federal criminal law, as embraced in the Senate side bill introduced in March of this year as S.2178 ("The Consumer Telephone Records Protection Act of 2006.) Absent that, the Committee might want to consider expanding the scope of the civil sanctions in the current bill to embrace private rights of action, including class action law suits, by victimized citizens.

I make these suggestions solely because of the first-hand experiences both I and my family have had as victims of this nefarious practice. Though I alone was targeted by these so-called pretexters (I prefer the more accurate and less sanitized phrase, "criminal impersonators") the activities they set in motion quickly enveloped my wife and our three children as well as myself. And during the four years that have followed, our lives have been convulsed in ways that set our nerves on edge even now, whenever the phone rings unexpectedly or at an odd hour in my home office.

To discover that someone has spent weeks trying to obtain access to you and your family's most personal and private records, and finally succeeded at it, is like learning that a Peeping Tom has been spending weeks on end hovering at night outside your bedroom window, watching and videotaping everything that goes on inside.

And it doesn't end there. When a pretexter goes unpunished, his victims can easily enough start to worry about things that never before concerned them – things they can ultimately do nothing about except worry even more, until all of life becomes a parade of imagined cvatastrophes. Is someone reading my mail? Is there a tap on my phone line? A bug in my bedroom?

These are not the sorts of questions that law-abiding Americans should be asking of themselves, but they arise easily enough when the digital Peeping Tom is discovered with his eye to the bedroom window, and a combination of weak laws, public apathy, and conflicted law enforcers allows him to escape.

In the 2003 U.S. Supreme Court case of *Lawrence et al v. Texas*, which overturned a Texas sodomy law, Justice Kennedy wrote, "Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct." But no such freedom can prevail in a world in which the theft of a person's telephone records is viewed as routine day-work by the private eyes who steal them, and is simply ignored by law enforcement.

Pretexting for financial records has already been outlawed by the Financial Services Modernization Act of 1999 (aka the Gramm-Leach-Bliley Act), which carries heavy criminal penalties for violators of certain of its provisions. The principles of law

and privacy imbedded in that Act need now to be extended to the the booming new business of digital Peeping Toms and phone records thieves.

My name is Christopher Byron, I am 61 years of age, and I have been a working journalist my entire professional life. I am a graduate of Yale College and the Columbia University School of Law. I have worked as a foreign correspondent and editor for *Time* Magazine, and as assistant managing editor for *Forbes* Magazine.

I have authored six books, one of which (*Martha Inc.*) was a New York *Times* bestseller and was made into an NBC Movie of The Week. A Russian language translation of my latest book, *Testosterone Inc., Tales Of CEOs Gone Wild* is scheduled to go on sale worldwide.

For most of the last twenty years I have also written weekly commentary columns on Wall Street and business for a variety of publications. It was in connection with one such column, written by me for *Red Herring* magazine and published in September of 2002, that I became the victim of a pretexting conspiracy to obtain my telephone business records.

The story that led to all this concerned a company in Vancouver, Canada called Imagis Technologies Inc., which claimed to be in the facial recognition software business. In the wake of the attacks of 9/11, the company began issuing press releases promoting its software products as weapons in the fight against international terrorism, and one of those press releases eventually crossed my desk.

Looking further, I learned that the chairman of the company was the recently retired deputy chief of the F.B.I., Oliver ("Buck") Revell, whose name I recalled from his involvement in the Pan Am 103 story, about which I had written extensively some years earlier.

Yet aside from the presence of Revell on the board, the Imagis operation seemed unimpressive in every way – a typical Vancouver penny stock featuring limited revenues along with a history of large and continuing losses, and a shaky balance sheet.

Two of the company's top officials particularly troubled me. One was the company's controlling shareholder – an individual named Altaf Nazerali -- who had already been linked in the Canadian press to the European operations of a notorious U.S. stock swindler named Irving Kott in the 1960s. Two decades later Nazerali's name surfaced as an alleged money courier in the infamous BCCI scandal.

When I asked Revell in an interview in late July of 2002 why he had agreed to serve as chairman for a company controlled by a man like Nazerali, he said he had arranged to have Nazerali "vetted" and that the man "had never been involved in unethical or illegal activity."

Revell was even more enthusiastic about the bone fides of an individual named Treyton Thomas, whom Revell had appointed to the Imagis board only weeks earlier, on July 9th. Thomas enjoyed bombarding the press with self-celebratory publicity releases about himself. In them he claimed to be the head of a $600 million offshore hedge fund called the Pembridge Group, to hold a degree from Harvard and so on and so forth. In an interview with one gullible reporter, he even boasted of having back-channel lobbying access to the White House and the Bush Administration.

Revell told me he had vetted Thomas as well, just as he had vetted Nazerali. But he certainly couldn't have done a very good job since utterly nothing Thomas claimed about himself was true. The so-called Pembridge Group hedge fund was nothing but a creature of Thomas's imagination. In short, it did not exist.

To help fool Revell into thinking otherwise, Thomas had leased some swanky Boston office space from a company that rents space by the day to traveling salesmen. But he needn't have bothered because Revell never visited the premises. And it's just as well for Thomas that he didn't because this was a $600 million hedge fund with no employees, no back office, not even any Bloomberg terminals.

It struck me as impossible for Revell not to have known all of this – especially when Thomas, just prior to being appointed to the Imagis board, orchestrated a much-publicized, but entirely fake buyout offer for Imagis through press releases issued by the non-existent Pembridge Group, then made a killing illegally from the resulting run-up in the shares that followed.

Weighing these facts, I wrote a fair but distinctly negative story on Imagis, asking why Revell, trained as he was in the dark arts of the FBI investigator, had permitted such things to unfold right under his nose. Two weeks later, both *Red Herring* and I were sued for libel by Imagis in a Vancouver court.

Being sued for libel is a traumatic experience for anyone, and this situation was even worse since the suit had been filed in a Canadian court, where libel laws are different from those in the U.S., thus affording defendants none of the normal Constitutional protections available to defendants in U.S. actions.

Bad as that was, it got unexpectedly and immeasurably worse when, several weeks later, in the late afternoon of October 16, 2002, my home office telephone rang and my wife, Maria, who works as my research assistant and office manager, answered it and thereupon found herself in conversation with a person who purported to be a customer service representative from AT&T, our long distance phone carrier.

Sitting at my desk nearby and absorbed in my own work, I paid no attention to the conversation that followed – though I did detect a certain wariness begin to creep into her voice as the conversation continued. A moment or two more passed and then suddenly she shrieked into the phone: "What?" and began stammering, "That's a lie! I've done no such thing!"

It seemed that the AT&T Customer Service rep had called up to check on some problems we were apparently having obtaining copies of our July 2002 phone bill. In fact, we had been having no such problem and had never contacted AT&T about it at all.

Yet AT&T's computer logs appeared to show otherwise. The logs showed that, beginning on August 1, 2002 – mere days after I had interviewed Revell and finished writing my story, and twelve days before *Red Herring* received its first law suit threat-letter from Imagis – AT&T's Customer Service Dept. began receiving telephone calls from persons claiming to be the AT&T customer for the account, seeking information of one sort or another about the account. Sometimes the caller would impersonate either me or my wife directly; on other occasions the caller would use a fake name such as "Jackie Byron" or vaguely, "Lynn."

These calls went on without letup for 10 full weeks, sometimes at a rate of two and three a day, until they totaled an incredible 48 different contacts. Yet it wasn't until October 15 when the impersonator/pretexters at last hit pay-dirt and got what they were after: access to our office phone records for the July 2002 billing period. That of course was the month during which I had interviewed Revell, submitted requests for interviews with Thomas and Nazerali (which were declined), and conducted other interviews for the story.

From research developed by the Subcommittee for these hearings, we now know that this practice is referred to among phone records thieves as "dialing for dummies," and basically amounts to a kind of craps shoot in which the pretexter phones up Customer Service "800 numbers" of telephone companies over and over again, trying one ruse after the next until he or she finally connects with a service rep gullible enough to swallow the bait and provide the information being sought.

In our case, the pretexting payoff came on Oct 15th when AT&T's internal log file of incoming calls to its customer service help number shows that a female impersonator claiming to be "Mrs. Byron" succeeded in convincing a customer service rep named Shakela Felton who was employed by an Irving, Tex-based AT&T subcontractor called Aegis Communications Inc., to pull up our July 2002 phone record to her computer screen and read aloud from it, one after the next, each and every one of 94 separate phone calls made from the phone during the month of July – a task that took more than a hour.

The AT&T log shows that soon afterward, a male impersonator claiming to be "Mr. Byron" called back, reached the same Aegis Customer Service Rep, Shakela Felton, who had answered the earlier call, and got that person to repeat the entire exercise all over again, which went on for yet another hour.

When I learned of all this I filed an immediate complaint with the FBI field office in Bridgeport, Conn., and simultaneously, a complaint with the FBI's financial crimes unit at the Bureau's national office in Washington. The officials with whom I spoke at

both locations expressed immediate interest in the matter. But as soon as I mentioned my suspicion that a recently retuired top FBI official named Revell might be implicated, their eagerness to help seemed to dissipate and they stopped returning my calls.

Officials at AT&T, where I also filed a complaint, expressed equally sincere-sounding interest in what had transpired. But they too subsequently proved to be persistently unhelpful, routinely providing evasive, non-responsive (and sometimes even contradictory) answers to my questions. For months I was kept in the dark as to what information they were even coming up with.

In May of 2003, -- and acting in response to the threat of a federal civil rights suit to be filed on my behalf by News Corp., owner of the *New York Post* where I am a columnist -- AT&T's chief counsel for consumer marketing, Michael C. Lamb, disgorged to me what he represented to be the internal investigative case file that AT&T had given to the FBI six months earlier in November of 2002. I have provided a copy of those documents to the Subcommittee.

The case file AT&T gave me was clearly sanitized when I received it, and was missing information vital to identifying the pretexter. An accompanying cover letter from Lamb brushed aside the missing materials as basically a clerical error and promised to pass them along to me subsequently, but he never did. Lamb has since left AT&T, and he has not been replaced. I have since requested the documents from AT&T directly, but so far the company has produced nothing.

In any event, the case file documents I did receive show AT&T's so-called investigation into my complaint to be haphazard, casual and effectively little more than a go-through-the-motions white-wash in which preposterously contradictory statements from those questioned in the probe were simply ignored – after which the whole file was tossed like a hot potato to the FBI and AT&T's own involvement in the affair ended.

For example, on November 8, 2002, AT&T's chief counsel, Lamb, participated in a lengthy three-party conference call involving himself, myself, and the AT&T security official who had been assigned to conduct the investigation, David Lankford. The purpose of the call: to keep me updated on the progress of the investigation.

In that call the question of AT&T's policy regarding the use of password protection on customer accounts came up. That policy is muddled and confusing and differs in several respects depending upon whether a person is trying to access phone records information online via the internet or orally over the phone with a customer service rep.

Because of the way the internet itself operates, in order to gain online access to the information in an AT&T customer's account it is necessary to know the secret customer-assigned password that supposedly protects the account from the snooping eyes of intruders.

But passwords are less important when it comes to protecting customer accounts from intrusion over the phone. That's because the customer service rep who winds up fielding the request can easily establish the identity of the caller by accessing the account and then asking the caller to answer questions related to information on the account itself.

As a result, AT&T leavers it the customers themselves to decide whether they want to add an additional level of protection to their phone records by using passwords to restrict access to them over the phone as well as via the internet.

In the November 8th conference call both Lamb and Lankford were emphatic and categorical that no customer service rep would provide account information over the phone to a caller by asking the person for the account's *online* password in order to establish his or her bone fides. "We would never ask for a password," said Lankford. "It would not have been consistent with our practice," added Lamb.

But when Lamb finally surrendered AT&T's case file to me the following May, it contained a handwritten statement from the service rep in the matter, Shakela Felton, revealing at a minimum that she had done precisely that.

In her statement Felton said that on October 15, 2002 she had read aloud the details of the July phone bill to the caller because that person had first provided her with the password to the account. ***Yet our account contained no such password for over-the-phone access at that time, and one wasn't added until late the next day (October 16th) when the theft was discovered and an AT&T official advised us to do so.***

Two days later, on Oct. 18th, the service rep., Felton, gave the first of three statements on the matter, followed by a second one on November 5th and a third on November 7th. In each statement she stuck by her story of having given the information to the caller only after the caller had provided her with the password to the account – a password that did not yet even exist.

Shakela Felton's shaky password story was only one of many things AT&T failed to pursue. They never addressed the utterly implausible coincidence whereby Felton received two back-to-back calls from the same pretexters on October 15th, each lasting more than an hour, and each concerned with the same subject (my July 2002 phone calls).

Nor did AT&T ever produce a satisfactory explanation as to why the company, with all its claimed cutting edge technology, proved unable to trace either call -- each lasting more than an hour -- back to its originating telephone. Week after week of insistent pressuring brought little beyond tech-world doubletalk and foot-dragging, ending finally when Lamb told me the company had traced one of the calls to the town of Alba, Texas, some 30 miles east of the Irving, Tex facility of AT&T's subcontractor, Aegis Communications, Inc., where Shakela Felton worked.

It took months and even years of nonstop investigation on my part before it became possible to glimpse even the outlines of what I had become caught up in, and many questions remain unanswered to this day. But the key facts are by now clear.

For starters, with the passage of time it has become increasingly obvious that the facts I had reported about Imagis Technologies Inc were all 100% true and accurate, and that the company's libel suit against me had been inspired entirely by the desire to discourage either *Red Herring* or any other publication from pursuing the matter any further.

The judgment of the market regarding this atrociously run company has been devastating. Since my article first appeared in September of 2002, Imagis's share price has fallen from $4 per share to a current price of less than 20 cents per share. Meanwhile, the company's revenues, never strong to begin with, have flat-lined while losses have soared out of sight. In June of 2005 the company changed its name to Visiphor Corp.

In the aftermath of the theft of my phone records, and with the FBI seeming to show no interest in the case, I filed a complaint against Imagis's rogue board member, Treyton L. Thomas, with the Enforcement Div. of the U.S. Securities and Exchange Commission's district office in Boston, where Thomas had run his pump-and-dump scam out of a rented office near Boston Harbor.

By August of 2003, the SEC had opened an investigation into Thomas's activities and begun seeking his books and records as well as those of a woman he was living with in Boston named Cheryl Stone. On August 28, 2003, I reported this fact in the New York Post along with much else of what I had learned about Thomas since my original story on the man had first appeared in *Red Herring* a year earlier.

Among the new revelations, which Revell had somehow managed to miss in his own vetting of the man, were these:

- That Thomas's so-called $600 million offshore hedge fund was actually nothing more than a six-employee electrical equipment supply shop that Thomas had been running as a sideline business in Atlanta, Ga. while he bounced from one brokerage firm job to the next.
- That Thomas had precipitated the breakup of the marriage of a well-known Atlanta, Ga. plastic surgeon and had run off with his wife, with whom he was now living in Boston.
- That for most of his life Thomas had been known as Tracey Lee Thomas and had traveled the world under a U.S. Passport that identified him as a woman.
- That while serving as an enlisted man in the U.S. Marines in Kenitra, Morocco in the 1970s, Thomas had carried on a torrid two-year love affair with an underage junior high school girl who was living with her family on the base, and finally
- That Thomas had previously been arrested (though not convicted) on felony fugitive charges in Georgia, and finally,

Soon after the *New York Post* reported these facts, Thomas's career as an outside member on Imagis's board of directors came to an abrupt end – without any public explanation for his departure.

One reason for the lack of disclosure may be the SEC investigation itself. In the course of the Thomas probe, SEC investigators had obtained Thomas's telephone records for the period that covered the autumn of 2002, and had thereafter issued a document production request to a Wall Street stockbroker whose own phone number had appeared as an outgoing call from Thomas's phone.

The broker was in fact a long-time confidential source of mine and I had spoken with him regularly over the years in the course of researching various Wall Street-related subjects. The broker did not know Thomas and had said so when I had mentioned Thomas's name to him during a phone call I had placed to him while preparing my September 2002 story for *Red Herring*.

So, when the broker received a letter a year later, in August of 2003, from the Boston District office of the SEC asking him to turn over all account records, trading tickets, statements and whatnot regarding one "Tracy (Treyton) Thomas ," the broker telephoned the Boston district office to ask why since he had no idea who the Thomas person even was. The investigator explained that the broker's phone number in New York had been called from Thomas's own phone in Boston, and the broker thereafter relayed that information to me.

This of course led to only one conclusion: Thomas had either obtained my purloined phone records himself, or someone else had given them to him. Either way, he had apparently gotten his hands on them somehow and had set out to phone up the numbers on the list to see who my sources for the *Red Herring* story had actually been.

As any journalist will tell you, the most valuable assets a reporter can have are his confidential sources, and to have the names of dozens of them suddenly drop into the lap of someone like the scruple-free Thomas was an appalling thought to say the least. What if the word began to get around that even Byron's most confidential sources risked turning up on the receiving end of a document production letter from the SEC? Who would return my phone calls then?

Obviously this was something I wanted to keep as tight a lid on as possible. But trying to do so seemed futile when, a week or so after the theft of my records, I received a telephone call from a top – though highly confidential – source in the hedge fund world.

The source knew nothing of what was going on between AT&T and me, and had phoned up to discuss something else entirely. Yet just as I had done with the Wall Street broker, I had also spoken with my hedge fund source about Thomas for my *Red Herring* story the year before, so his phone number had appeared on my July 2002 phone records.

As a result, one may easily enough imagine my alarm when the man proceeded to mention, in the course of our conversation, that he had recently experienced the oddest thing – then went on to describe how someone from AT&T had phoned his home only a day or two earlier to ask whether he had been having trouble accessing his phone records.

One does not need to behold the rotting corpse of Jimmy Hoffa to accept that Hoffa is actually dead, so I will say on the basis of all the foregoing that I do not need to possess a signed confession and a Polaroid snapshot showing Treyton Thomas caught in the act of pretending to be me to believe that he was mixed up one way or another in the theft of my phone records. And I also don't need any more than is already available on the public record to suppose that Revell either had a hand in it himself or chose to look the other way.

By the start of 2004 Thomas had left the Imagis board, and eleven months later, in in November of 2004, the SEC filed civil fraud charges against him for orchestrating his pump-and-dump scam in Imagis's stock. Eighteen months later, in May of this year, Thomas pleaded the civil law equivalent of *nolo contendere* and agreed to pay $282,400 in assorted fines and penalities, and promised never again in his life to serve as an officer or director of a public company, or to engage in or promote a securities offering.

Unfortunately, the SEC chose not to proceed against Thomas in the phone records matter, claiming the Commission lacked jurisdiction, and advised me to approach the FBI instead. Yet as we have seen, the FBI has done nothing either, and I doubt it will without aggressive pressure from the Congress.

There are plenty of reasons for the FBI to want to steer clear of this case, and the apparent involvement of Revell is only one of them. During a portion of the time that Revell served as a top official at the FBI, eventually acquiring the title of Associate Deputy Director, his counterpart at the Drug Enforcement Agency was an individual named Terrence M. Burke. Beginning his government career as a CIA intelligence officer in Southeast Asia in the 1960s, Burke moved later to the DEA where he eventually acquired the title of Deputy Administrator of the entire Agency. In that capacity he was in frequent collaborative contact with Revell, and the two men were regarded in law enforcement circles as friends.

In 1991 Burke left the government, joined a Washington D.C. firm of private investigators (The Investigative Group Intl.) and eventually left to launch his own firm, T.M. Burke International, in Colorado, at the end of the 1990s. In that capacity he turned up in Vancouver in the summer of 2002, where he tried to gain the confidence of a local business reporter by claiming that he had been hired by an unidentified client in Europe who was "seeking revenge" on Imagis's controlling shareholder, Altaf Nazerali – not revealing of course that Burke himself was a long-time, top level associate of Revell's in U.S. law enforcement and that Revell was presumably privy to vastly more dirt on Nazerali than was a local business reporter who had never even met Nazerali.

Beyond the apparent involvement of Revell and the possible involvement of Burke looms a vast array of other matters that would help discourage an FBI investigation into the theft of my phone records.

The AT&T subcontractor where Shakela Felton worked – Aegis Communications Inc. – is in the so-called outsourcing business, which means it handles back-office matters such as customer accounts management and the staffing of call centers for well-known corporate clients ranging from AT&T to American Express, Discover, and others.

Over the years, Aegis has figured in several high-profile identity theft cases, including a much-publicized case in which a ring of Detroit area identity thieves paid Aegis phone reps to steal the credit card information of more than 2,300 American Express cardholders, then used the information to bilk Detroit area merchants out of an estimated $14 million in merchandise charged to the accounts then sold on the black market.

As the Subcommittee's research has revealed, many in law enforcement at every level of government now routinely obtain the telephone records of investigative targets, while keeping their own fingers clean by hiring pretexters to do the dirty work for them. Companies such as Aegis are an attractive place for pretexters to go fishing, and because of that fact alone it seems unlikely that federal investigators would eagerly embrace the idea of digging into the sieve-like nature of Aegis's security procedures on behalf of corporate clients whose computers bulge already with the accumulated personal and financial records of virtually the entire American public. No one welcomes investigating a former colleague, in government or anywhere else – and that is certainly true when an investigation can undercut post-government business opportunities for the retired investigator.

Outsourcing shops like Aegis are one of the weakest links in the chain of custody over the financial and personal records of the American people. It is fine to stress the importance of the U.S. Patriot Act and the need to crack down on financial fraud in the war on terrorism. But that is hardly enough when any enterprising group of terrorists with the desire to do so could quietly acquire control of an outsourcing shop like Aegis, move it abroad to a place like India, where operational oversight of such companies by the government is limited at best, and then begin the wholesale downloading of America's consumer records database.

This is no idle speculation either. In September of 2003, at just the time the SEC had begun pursuing its investigation of Thomas, a U.K.-based outsourcing company called Allserve Systems Ltd. announced plans to acquire Aegis from the Washington D.C. investment fund that was Aegis's controlling shareholder, Thayer Capital Partners. But who owned Allserve? Not even the top officials at Aegis seemed to know.

Yet by this time I was deeply immersed in researching everything possible regarding Aegis and the theft of my phone records, and by tracing out the evolution of the U.K.-based company in business databases around the world, I was able to establish that

the man behind the planned purchase was an financier named Dinesh Dalmia, who was busy building up a Calcutta-based outsourcing business for corporate clients in the U.S., the U.K. and elsewhere.

But there was more to Dalmia than just that. Further research revealed that Dalmia was actually an international financial fugitive, who had recently fled India and was now roaming the earth with a worldwide Interpol "Red Corner" arrest notice over his head for crimes that ranged from money laundering and forgery to stock market fraud.

And there was more. From a confidential source in India I obtained e-mail traffic between Dalmia and an associate in the United Arab Emirates in the days following the terrorist attacks of 9/11. In those e-mails Dalmia and his man in the Gulf discussed plans to sell the Iraqi Ministry of Defense an array weapons-related computer programs, including a package of software tools for managing a biological warfare campaign.

Before publishing these facts I asked a spokesman for Thayer Capital just how thoroughly the investment group had checked out Allserve Systems Ltd. before agreeing to sell it majority control of an outsourcing company that enjoyed routine access to some of the most sensitive and private consumer information in the country. I was told that Allserve was a fine company and basically to mind my own business.

I also got no where when I asked for interviews with anyone on Thayer's blue-ribbon "advisory board," which boasted names like those of former Secy. of Defense William Cohen, Clinton Administration adviser Vernon Jordan, ex-head of Housing and Urban Development Jack Kemp, and the former chairman of American Express James Robinson.

I explained to the Thayer spokesman that I wanted to know if any of these luminaries had heard of Dinesh Dalmia and whether they were aware that he was behind the Allserve acquisition and that he planned to hold the Aegis shares in an anonymous nominee account in the tax haven island nation of Tortola. To these questions I received no answers at all.

I published these facts in the *New York Post* and the deal quickly fell apart – though not before both the newspaper and I received a retraction demand and libel lawsuit threat letter from a lawyer in New Jersey who claimed to represent Dalmia. The lawyer asserted that it was libelous to have reported that Dalmia had tried to negotiate the sale of a germ warfare software package to Iraq because, as the lawyer put it, "no such contract was ever executed."

The *Post*'s general counsel replied in a rebuttal letter that we intended to retract nothing, and that was the last we heard from this particular lawyer regarding Dalmia.

Two years later Dalmia resurfaced, once again hidden behind his Allserve Systems mask and further protected this time by what amounted to a new defensive perimeter of offshore shell companies.

Dalmia's goal, once again, was to take over control of a U.S. outsourcing company – in this case employing a convoluted scheme involving an array of companies in New Jersey that he secretly controlled and intended to merge with a NASDAQ-listed outsourcing company called the A Consulting Team Inc.

Extensive reporting by the *Post* caused this deal as well to fall apart. And when the *Post* reported, based on a search of public land records in New Jersey, that this international fugitive, presumably hunted by Interpol wherever he went, was in fact living the life of Riley in a Fort Lee, N.J. mansion overlooking Manhattan, we received a second libel threat letter.

This time the threat came by way of a lawyer better known for his criminal defense work than for his acumen in the law of defamation and libel: Atty. Lawrence Barcella of Washington. Barcella claimed the *Post's* coverage of Dalmia was a tissue of lies and distortions but failed to cite any evidence to support the assertion. Once again the *Post* replied that we would retract nothing, and it was the last we heard from Barcella as well.

In January of 2006 Dalmia fled the U.S., one step ahead of the FBI, leaving behind a trail of personal aliases, false and forged financial statements, fake invoices, and bogus bank accounts in the names of non-existent companies. He had used these tools to swindle some of the most prestigious – and presumably savvy --financial institutions in America out of an estimated $130 million in computer leasing deals.

When Dalmia defaulted on his loan payments in the deals and the creditors moved to repossess the computer equipment that collateralized the leases, they discovered that the equipment had already been shipped to India and sold. When they demanded to see the supporting paperwork they were told they could not. Reason: a sinkhole had opened in downtown Calcutta and swallowed up all the records.

Dalmia's network of fraud – all of it based on front companies in the outsourcing business – stretched from Singapore to the U.S. to London and beyond. And it all ran the same way, at the same time in one country after the next. When Britain's Serious Frauds Office arrived at the doorstep of Dalmia's front operation in London to ask some questions, they found the offices deserted and the files in a shambles. Reason: the staff had headed for Heathrow airport and returned to India.

Much as Dalmia's creditors may have felt they had been dealing with a ghost, the Indian swindler was real enough, and in early February of this year he was arrested by Indian government agents who had been tipped that he had reentered the country by crossing over from Nepal and was staying with relatives in New Delhi.

Dalmia's arrest and subsequent detention, which continues to this day, proved a sensation in India, with the media exploding in seemingly nonstop coverage of each new charge the authorities have lodged against him – most of which relate to his role in a

series of late 1990s stock swindles that climaxed in the collapse of the Calcutta and Bombay Stock exchanges.

Yet except for coverage in the *New York Post*, Dalmia's three-year crime spree has received almost no attention at all in the U.S. – highlighting another of the many ways in which phone records thievery imperils all Americans. Dalmia didn't simply try to steal the phone records of one or two individuals, he tried to steal an entire company stuffed to the gills with the phone and financial records of Americans by the millions… and he nearly succeeded.

So I commend the Subcommittee for its efforts on behalf of H.R. 4943, and urge only that you stay mindful of the broad and encompassing risks posed by phone records thievery in all its many forms. Stealing one person's phone records is bad enough. This nation should not be at constant risk from scoundrels eager to steal the phone records of everybody, all at once.

Thank you for your time. Respectfully, Chris Byron